

**COMMONWEALTH OF MASSACHUSETTS
DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY**

PETITION FILED BY VERIZON
MASSACHUSETTS FOR A WAIVER OF
CERTAIN SERVICE QUALITY RESULTS
MEASURED UNDER THE PERFORMANCE
ASSURANCE PLAN FOR JANUARY 2003

D.T.E. 03-38

COMMENTS OF AT&T COMMUNICATIONS OF NEW ENGLAND, INC. ON VERIZON
MASSACHUSETTS' PETITION FOR A WAIVER OF CERTAIN SERVICE QUALITY
RESULTS MEASURED UNDER THE PERFORMANCE ASSURANCE PLAN FOR
JANUARY 2003

Jay E. Gruber, Esq.
Jeffrey Fialky, Esq.
AT&T Communications of New England, Inc.
99 Bedford Street, 4th Floor
Boston, MA 02111
(617) 574-3149 (voice)
(617) 574-3274 (fax)

April 10, 2003

TABLE OF CONTENTS

INTRODUCTION.....	1
ARGUMENT.....	3
I. THE WAIVER PETITION FAILS TO PROVIDE EVIDENCE SUFFICIENT TO MAKE A <i>PRIMA FACIE</i> SHOWING THAT RELIEF IS JUSTIFIED, AND SHOULD BE DISMISSED.	3
A. The Waiver Provision Upon Which Verizon Relies Requires Demonstration Of Events Of An “Extraordinary Nature,” That Are “Beyond Verizon’s Control,” And That Could Not Be Prevented By “The Company’s Normal, Reasonable Precautions For Difficult Situations.”	3
B. Verizon’s Petition Identifies The Evidence That It Should Have, But Did Not, Present And, Therefore, Should Be Dismissed For Failure To Make A Prima Facie Showing.	4
II. VERIZON COULD HAVE REASONABLY PROTECTED ITSELF, AND THEREBY PROTECTED THEIR WHOLESALE CUSTOMERS, AGAINST HARM BY THE SLAMMER WORM.	8
III. PENDING A DEPARTMENT RULING ON THE PETITION, THE DEPARTMENT SHOULD REQUIRE VERIZON TO FILE THE MAY 2003 PAP RESULTS ASSUMING THE PETITION IS NOT GRANTED.	13
CONCLUSION	14

Introduction

Pursuant to the request for comments issued by the Department of Telecommunications and Energy (“Department”) on March 27, 2003, AT&T Communications of New England, Inc. (“AT&T”) hereby comments on the Petition (“Waiver Petition”) of Verizon Massachusetts (“Verizon”) For A Waiver Of Certain Service Quality Results for January 2003 Under the Performance Assurance Plan (the “PAP”), dated March 18, 2003. Verizon requests that the Department waive penalty payments owed to CLECS under the Massachusetts PAP, claiming that the service disruptions caused by the “slammer worm” computer virus were beyond its control and therefore should be exempted from the PAP.

The Petition should be rejected on several grounds: First, Verizon has failed to provide sufficient evidence to make a *prima facie* showing that relief is warranted, as expressly required by the PAP. Second, the Verizon Waiver Petition should be denied on the merits, because the evidence demonstrates that the effect of the slammer worm virus on Verizon’s performance was easily preventable by a simple software patch (a) that had been available to Verizon for six months and (b) that had been highlighted as critical by Microsoft for protecting against just this type of virus. One of the largest telecommunications companies in the world should not be excused for its failure to perform basic software patch management, especially when its wholesale customers and their end users bear the negative effects of Verizon’s irresponsible oversight. There is no authority to which they can turn to be excused from the results of Verizon’s mismanagement.

Under the PAP, Verizon must provide evidence sufficient to make a *prima facie* showing that relief, *i.e.* service quality waiver, is warranted.¹ As set forth below, Verizon's submission fails to make such a showing. Indeed, as explained below, Verizon's own Waiver Petition specifies the showing that Verizon should have made and graphically demonstrates the evidence missing from Verizon's presentation. Accordingly, the Department can and should dismiss the Waiver Petition outright.

If, however, the Department chooses to rule on the merits of the Waiver Petition, Verizon's failure to meet the performance metrics under the PAP is inexcusable, and should not be waived. Verizon's argument that the specific slammer worm virus is an extraordinary and unpredictable event is beside the point. The real point is that the vulnerability exploited by the slammer worm virus had been identified by Microsoft six months earlier, when Microsoft had provided a software patch to protect against a computer virus that would exploit that vulnerability. The Slammer Worm virus was a disaster waiting to happen for any company that failed to take simple, inexpensive steps to protect against a known vulnerability. Verizon's wholesale customers have already suffered the consequences. Verizon should not be excused from the consequences of its own behavior.

¹ PAP, at 20.

Argument

I. THE WAIVER PETITION FAILS TO PROVIDE EVIDENCE SUFFICIENT TO MAKE A *PRIMA FACIE* SHOWING THAT RELIEF IS JUSTIFIED, AND SHOULD BE DISMISSED.

A. THE WAIVER PROVISION UPON WHICH VERIZON RELIES REQUIRES DEMONSTRATION OF EVENTS OF AN “EXTRAORDINARY NATURE,” THAT ARE “BEYOND VERIZON’S CONTROL,” AND THAT COULD NOT BE PREVENTED BY “THE COMPANY’S NORMAL, REASONABLE PRECAUTIONS FOR DIFFICULT SITUATIONS.”

The Department well appreciates that Verizon’s OSS performance is crucial to the development and expansion of local exchange competition. In adopting the Massachusetts PAP, the Department’s intent was to ensure that Verizon had the appropriate incentives to take whatever measures are necessary “to prevent . . . serious degradation in the quality of wholesale service provided to competing carriers.”² In this regard, the Department sought to impose reasonable penalties that would give Verizon the incentive to undertake *proactive* measures to assure quality wholesale performance. The objective was to make the penalties for poor performance more than just a cost of doing business for Verizon.

Thus, the Massachusetts PAP was designed to ensure that CLECs are entitled to substantial bill credits when Verizon fails to meet the Method-of-Entry Measures and Critical Measures. These bill credit remedies have been triggered in the instant case. There is no dispute here that Verizon failed to meet Method-of-Entry Measures for both UNEs and for Resale, and failed to meet a Critical Measure for OSS Interface Availability.³ As a result of these failures, Verizon owes substantial preliminary bill credits to CLECs including AT&T.

² D.T.E. 99-271 (Sept. 5, 2000), at 1.

³ Waiver Petition, at 1.

Verizon seeks to avoid these bill credits by requesting a waiver pursuant to the “third ground” of Section II(j) of the PAP.⁴ The waiver provision relied on by Verizon is, for good reason, exceedingly strict, both in terms of the truly exceptional events required to be shown and the demanding standard of proof of those events that must be satisfied by Verizon. In particular, the PAP contemplates the possibility of a reduction of owed bill credits for failure to satisfy certain performance standards, including those related to vital OSS functions, only where Verizon demonstrates that events are of an “extraordinary nature,” that are “beyond Verizon’s control,” and that could not be prevented by “the company’s normal, reasonable precautions for difficult situations.”⁵

B. VERIZON’S PETITION IDENTIFIES THE EVIDENCE THAT IT SHOULD HAVE, BUT DID NOT, PRESENT AND, THEREFORE, SHOULD BE DISMISSED FOR FAILURE TO MAKE A PRIMA FACIE SHOWING.

Pursuant to the PAP, Verizon must make a *prima facie* case in its Waiver Petition that the service disruptions resulting from the Slammer Worm event were beyond its reasonable control.⁶ In actuality, the event that Verizon claims was “beyond its control” is its own failure to deploy a readily available software patch. In its Waiver Petition Verizon’s purported rationale for failing to install the software patch includes a description of the challenges of “patch management,” *i.e.* that the decision of whether or not to install a patch is based upon consideration and counterbalancing of the pros and cons.⁷ This very rationale, however, clearly demonstrates that Verizon’s decision not to install a patch in the present case was a *choice*, not something beyond

⁴ Id., at 1, 8-12.

⁵ PAP, at 20-21.

⁶ Id., at 21.

⁷ Waiver Petition, at 6-8.

Verizon's control. Moreover, Verizon's Waiver Petition details the analysis that Verizon goes through in order to make that choice and then *fails to provide a single shred of evidence that it undertook the analysis or investigation necessary to make the choice*. In short, as explained below, Verizon failed to provide any evidence that it took "normal, reasonable precautions for difficult situations."

In its Waiver Petition Verizon describes its "normal practices of maintaining the software infrastructure [which] include the process for obtaining, evaluating, testing and then deploying "fixes" or improvements to software components across its various systems."⁸ Verizon claims that it "is a complex and time-consuming function,"⁹ which apparently involves "a significant amount of interoperability testing and broad-based user experience."¹⁰ Verizon further claims there are a number of considerations that should be taken into account as part of any good process of patch management:

Further, a security patch for a given software component may require, as a pre-condition to deployment, the installation of prior patches or intermediate releases having nothing at all to do with security, and/or it may require the installation or upgrade of a companion software component (for example, a given version of MS SQL Server will require a given version of Windows NT). Finally, the downtime associated with the application of a specific patch (and any related upgrade or other patches) can be substantial and must be efficiently managed, especially in a business such as Verizon's with thousands of systems, and the large number of wholesale customers that interface with Verizon's systems.¹¹

⁸ Waiver Petition, at 6.

⁹ Waiver Petition, at 6.

¹⁰ Waiver Petition, at 7.

¹¹ Waiver Petition, at 7.

Given the detail with which Verizon has described its process of analyzing and determining the advisability of installing a patch, one would expect some evidence in the Waiver Petition that Verizon undertook this analysis. One would have expected, moreover, evidence that, on the basis of this analysis, Verizon had concluded that the patch provided by Microsoft, which Microsoft itself identified as “critical,”¹² should nevertheless not be installed. One would expect to see copies of contemporaneously prepared documents, memos, and analyses documenting the extensive testing and investigation that Verizon undertook and explaining the reasons why Verizon did not install the patch. At the time that the Slammer Virus hit in January, 2003, six months had passed since Microsoft issued the first patch in July, 2002, certainly sufficient time for a quite thorough analysis. Verizon, however, presented no evidence (a) that it had tested “interoperability” of the patch, (b) that it had considered the amount of “down time” involved in installing the patch, (c) that it had investigated whether “the installation of prior patches or intermediate releases were required” or “the installation or upgrade of a companion software component was required,” or (d) that the amount of time required to test and apply this patch was unreasonable given the amount of time necessary to test and apply the supposed “thousands” of other software patches potentially required.

Clearly, the Department noticed the stark failure of proof in Verizon’s Waiver Petition. In its discovery requests to Verizon, issued on April 3, 2003, the Department asked Verizon whether it followed its “patch management policy with regard to patches that address the vulnerabilities exploited by the Slammer Worm”¹³ and asked when Verizon first became aware

¹² See, discussion, *infra*, at 10-11

¹³ DTE-VZ-1-14.

of the patch.¹⁴ The Department is asking the right questions. It was Verizon's responsibility, however, to provide the answers to these questions in its Waiver Petition and to provide appropriate documentation in support. That responsibility is established by the express terms of the PAP which states that "[i]nsufficient filings may be dismissed for failure to make a *prima facie* showing that relief is justified."¹⁵

Indeed, the provision requiring a *prima facie* showing is an important part of the PAP. The requirement of such a showing enables a waiver petition to be addressed expeditiously, which preserves the "self-executing" characteristic of the PAP. In its approval of Verizon's New York Section 271 petition and implicitly the New York PAP upon which it was based, the FCC stated:

We recognize, however, that several commenters, as well as the Department of Justice, expressed considerable concern that the "exceptions" or "waiver" process built into the Plan could effectively destroy the self-executing aspect of the plan and open the door to extensive delay and litigation. We agree that a waiver process, if not narrowly limited to a discrete set of circumstances and subject to time constraints, could have such an impact.

The New York Commission has explained that it will consider waiver requests only in "limited, extraordinary circumstances." Second, the New York Commission placed time limits on the resolution of waiver requests, which will help to ensure that the Plan functions in a timely and predictable manner.¹⁶

¹⁴ DTE-VZ-1-15.

¹⁵ PAP, at 23.

¹⁶ *In the Matter of Application by Bell Atlantic New York for Authorization Under Section 271 of the Communications Act To Provide In-Region, InterLATA Service in the State of New York*, CC Docket No. 99-295, Memorandum Opinion and Order (released December 22, 1999), at 219, para. 441.

Moreover, these considerations were important to the Department, which cited with approval the foregoing language of the FCC's New York Section 271 order.¹⁷

If Verizon were allowed now to supplement its Waiver Petition with material it should have provided in the first instance, it would render moot the requirement that Verizon make out a *prima facie* case in its initial filing. It then creates a process that undercuts the self-executing nature of the PAP. Moreover, if Verizon submits written answers to the Department's questions with no supporting documentation, it raises serious questions as to the reliability and veracity of the responses. Such responses would need to be tested with further process. At a minimum, CLECs would need to have an opportunity to respond. Such a further response would not be required if Verizon had satisfied the PAP's requirement that it submit the necessary proof with its initial filing. While the Department's questions are the correct ones, the Department's need to ask them after Verizon omitted the information from its initial filing demonstrates that Verizon failed to meet its burden under the PAP. Verizon's Waiver Petition should be dismissed for failure to make out a *prima facie* case.

II. VERIZON COULD HAVE REASONABLY PROTECTED ITSELF, AND THEREBY PROTECTED THEIR WHOLESALE CUSTOMERS, AGAINST HARM BY THE SLAMMER WORM.

Should the Department consider Verizon's Waiver Petition on its merits, it should find that Verizon has failed to meet the stringent burden of proof required under the PAP. In fact, upon examination of the evidence set forth by Verizon, its claims and proof fall far short. Verizon's basic defense of its actions is that it was reasonable for it to do nothing in advance to address a known software vulnerability, because it would have been challenging to acquire,

¹⁷ D.T.E. 99-271 (Sept. 5, 2000), at 31.

install, test, and deploy a preventative software patch that the Company admits was generally available.¹⁸

In order to qualify for a waiver, Verizon must demonstrate “clearly and convincingly the extraordinary nature of the circumstances involved...and why Verizon’s normal, reasonable preparations...proved inadequate...”¹⁹ The Department found that the “clear and convincing” legal standard that Verizon must meet is an important part of the PAP, which gave the Department confidence that the waiver petition could not be abused.²⁰ The extra layer of protection provided by the “clear and convincing” standard is well established in Massachusetts jurisprudence. Courts have held that clear and convincing proof involves a degree of belief greater than the usually imposed burden of proof of “by a fair preponderance of the evidence.”²¹ In fact, the proof must be “strong, positive, and free from doubt.”²² Verizon has failed to provide any evidence to support its Waiver Petition that would meet even a lesser standard- much less the higher standard required by the PAP.

In its Waiver Petition, Verizon attempts to portray the challenges of “patch management,” and rationalizes its failure to install the patch in this case accordingly.²³ In fact, Verizon does not make any allegation in its Waiver Petition that it made an effort to actually

¹⁸ Waiver Petition, at 6-8.

¹⁹ PAP, at 21.

²⁰ D.T.E. 99-271 (Nov. 21, 2000), at 12.

²¹ *Stone v. Essex County Newspapers*, 367 Mass. 849, 870; 330 N.E.2d 161, 175 (Mass. 1975).

²² *Id.*

²³ Waiver Petition, at 6-8.

acquire, install, and test the software patch prior to January 25, 2003.²⁴ Verizon has not shown by any standard of proof -- let alone clear and convincing proof -- how challenging it would have been for Verizon to test and deploy the patch prior to that date. To the contrary, the fact that Verizon was able to test and deploy the patch in less than two days after the incident²⁵ strongly suggests that it could have deployed the software patch in a relatively short period of time before the incident if it had chosen to do so.²⁶ Verizon's boasts about the speed with which it delivered its cure *post facto*, evidences how painless the ounce of prevention would likely have been.

Verizon seeks to support its argument on the fact that companies with computer systems may find it difficult to be "100%-patched" at all times -- that is, to have all computer systems protected immediately with the latest software patches.²⁷ This claim fails in this instance, especially considering the foresight and diligence of Microsoft® -- the maker of the SQL Server 2000 and Microsoft Desktop Engine 2000 software affected -- in issuing patches for its software in this instance.

Microsoft, as a matter of policy, proactively solicits information on vulnerabilities in its software, and regularly notifies users, including IT professionals, of potential vulnerabilities

²⁴ Waiver Petition, at 7. ("Unfortunately, when the Slammer Worm hit, there were servers in Verizon...that had not yet received a patch to fend off the Slammer Worm.")

²⁵ Waiver Petition, at 4 ("From early morning Saturday, January 25, 2003, through late afternoon Sunday, January 26, 2003, Verizon proceeded to meticulously inspect, identify and remove infected devices, and where appropriate *patch*, test and reconnect devices[.]") (emphasis added).

²⁶ In fact, Verizon did much more than simply test and deploy the software patch where necessary in the 40-hour period beginning at 1:00 a.m. EST on January 25, 2003. Verizon also detected network flooding, identified the sources of traffic generation, isolated and quarantined its internal data networks, quarantined external networks, brought down four separate wholesale interfaces, notified CLECs by e-mail and by phone, and identified and removed infected devices, in addition to incrementally deploying the patch. Waiver Petition, at. 4-5. Merely testing and deploying the patch would have taken Verizon considerably less than two days.

²⁷ Waiver Petition, at 10-11.

through what are known as Security Bulletins.²⁸ Recognizing that not all vulnerabilities have an equal impact on all customers, Microsoft uses a four-part rating system for Security Bulletins. Security Bulletins with a “Critical” rating are deemed the most serious, precisely because the vulnerability “could allow the propagation of an Internet worm without user action.”²⁹ Next in gravity are Security Bulletins with an “Important” rating, reflecting vulnerabilities that “could result in compromise of the confidentiality, integrity, or availability of users’ data, or the integrity or availability of processing resources.”³⁰ To assist IT professionals and others in evaluating the deployment of patches for its software, Microsoft provides further guidance. In particular, Microsoft states: “We believe that customers that use an affected product should almost always apply patches that address vulnerabilities rated ‘critical’ or ‘important.’ Patches rated ‘critical’ should be applied in an especially timely manner.”³¹

Microsoft originally posted Security Bulletin MS02-039-- which identified the vulnerability ultimately exploited by the Slammer Worm and made available a preventative software patch -- on July 24, 2002 -- *six months* prior to the incident.³² Microsoft posted Security Bulletin MS02-056, which contained additional fixes for security vulnerability on October 2, 2002.³³ Moreover, Microsoft made available another patch -- which addressed the Slammer Worm vulnerability and additional vulnerabilities -- on October 16, 2002 -- more than

²⁸ See, <http://www.microsoft.com/technet/security/policy/rating.asp>.

²⁹ See, *id.*

³⁰ See, *id.*

³¹ See, *id.*

³² See, <http://www.microsoft.com/technet/security/bulletin/MS02-039.asp>.

³³ See, <http://www.microsoft.com/technet/security/bulletin/MS02-056.asp>.

three months prior to the incident.³⁴ The Security Bulletins were rated “Critical,” and were specifically directed to “Systems administrators.” While a reasonable person would have tested and deployed the first patch, and certainly would have tested and deployed the second and third, Verizon concedes it never tried to deploy any of the patches -- letting months pass in the interim.³⁵ This imprudent decision is the crux of the instant waiver, and it is the reason that the Department should deny the Waiver Petition on the merits.

Demonstrating just how unreasonable this delay was from an IT perspective, Microsoft warns in its explanation of its rating system – as if speaking directly to Verizon about this incident – that “attacks that impact customers’ systems rarely result from attackers’ exploitation of previously unknown vulnerabilities. Rather...attacks typically exploit vulnerabilities for which patches have long been available, but not applied.”³⁶ Far from being uncertain about the priority that should have been given to applying the patch that would have prevented the incident, Verizon completely ignored an urgent warning about the vulnerability of the software in question.

Verizon also makes broad and generally unsubstantiated claims about the experience of other companies with the Slammer Worm.³⁷ These claims, even if substantiated, are irrelevant to the waiver provision of the PAP, which is directed toward events that are truly exceptional and beyond Verizon’s control. What is most relevant is that Verizon had multiple notices and warnings from Microsoft regarding the availability of the patch, and failed to act on them.

³⁴ See, <http://www.microsoft.com/technet/security/bulletin/MS02-061.asp>.

³⁵ Had Verizon deployed both properly, the second would by design have superseded the first.

³⁶ See, <http://www.microsoft.com/technet/security/policy/rating.asp>.

³⁷ Waiver Petition, at 3.

Preventing harm from the Slammer Worm was certainly well within Verizon's control had it acted by installing the patch. Moreover, for its part, AT&T can say that it did not experience problems of the kind that Verizon experienced. Services to AT&T's wholesale customers such as ATM, Frame Relay, hosting, and wholesale voice were not materially impacted, nor were there any material impacts to AT&T's command and control systems, internal computing network, or customer care services similar to those of Verizon that were affected.

Verizon itself has recognized in other proceedings that Critical Measures reflect the availability of individual functions that, by themselves are so vital, they are "critical to the CLECs' ability to compete."³⁸ Testing and deploying software patches that protect the availability of these functions should be a first priority of Verizon. Under the basic provisions of the PAP, Verizon has an incentive to do so. But this is the very incentive that Verizon seeks to remove by requesting a waiver here. The Department should not undermine its own framework for ensuring CLECs have an effective opportunity to compete by allowing Verizon to do so.³⁹

III. PENDING A DEPARTMENT RULING ON THE PETITION, THE DEPARTMENT SHOULD REQUIRE VERIZON TO FILE THE MAY 2003 PAP RESULTS ASSUMING THE PETITION IS NOT GRANTED.

In its Waiver Petition, Verizon had asked the Department to issue a ruling on it by April 18, 2003 in order to meet the May 1, 2003 due date for process of January 2003 bill credits under the PAP. In its March 27, 2003, request for comments, the Department asked the parties to

³⁸ New York Public Service Commission, Case 97-C-0271, Pre-Filing Statement ("PFS") of Bell Atlantic - New York, p. 35.

³⁹ Indeed, the only way to avoid a myriad of after-the-fact questions about why Verizon chose to turn down or not to turn down various wholesale and retail OSS systems in the wake of a computer virus is to maintain rules that require Verizon to take action to protect wholesale OSS systems when, as here, it is possible. Moreover, the Department should recognize that it cannot determine the parity effects of Verizon's actions here (on, for example, pre-ordering availability) because a direct Verizon retail analogue does not exist (since Verizon does not access pre-order information through an interface as do CLECs).

comment on how the Department should treat the May 2003 PAP results, if it is unable to render a decision by April 18.

In order to avoid the concern of the FCC regarding the potential for delay in bill credits created by the filing of a waiver petition, the Department should require Verizon to file its May 2003 results assuming that the Petition is not granted, subject to true up in the unlikely event that the Department later grants the petition. In its approval of Verizon's Section 271 petition in New York, the FCC relied on the New York Public Service Commission's expressed willingness to resolve waiver petitions prior to the scheduled payment date.⁴⁰ The FCC's primary concern was that the "bill credits due for poor performance in a given month will never be 'stayed' by a waiver petition."⁴¹ If the Department does not render a decision by April 18, the Department can achieve that same result here only by requiring Verizon to file the May results assuming the Waiver Petition is not granted

Conclusion

It is not sufficient for Verizon to claim that because this was the first time in the history of the PAP that a virus or worm has impacted their service to CLECs, therefore it was an extraordinary event that justifies a waiver of its PAP obligations. The critical fact is that the vulnerability that the slammer worm computer virus exploited in Verizon's system was known and a fix had been available for six months. Indeed, Verizon had been warned by its vendor, Microsoft, that the problem in its system constituted the highest level of vulnerability making it

⁴⁰ *In the Matter of Application by Bell Atlantic New York for Authorization Under Section 271 of the Communications Act To Provide In-Region, InterLATA Service in the State of New York*, CC Docket No. 99-295, Memorandum Opinion and Order (released December 22, 1999), at 220, n. 1357.

⁴¹ *Id.*

“critical” that Verizon install a patch to protect against precisely the type of computer virus at issue in this Waiver Petition.

The Slammer Worm simply caught Verizon flat-footed, and revealed the company’s failure to proactively ensure its service quality obligations under the PAP. Moreover, the Department should not grant this Waiver Petition on a promise from Verizon “to do better next time.” Only real incentives, such as the penalty payments provided by the PAP, will motivate Verizon “to do better next time.” Accordingly, for the reasons set forth above, the Department should reject the Waiver Petition.

Respectfully submitted,

**AT&T COMMUNICATIONS OF
NEW ENGLAND, INC.**

Jay E. Gruber, Esq.
Jeffrey Fialky, Esq.
AT&T
99 Bedford Street, 4th Floor
Boston, MA 02111
(617) 574-3149 (voice)
(617) 574-3274 (fax)

April 10, 2003